

Privacy Policy Autom8

Last Updated: [Last Update Date]

The Autom8 Extension ("the Product") is a Tableau extension that enables dashboard viewers to send data directly from their browser in Tableau to a third-party platform via a configured n8n webhook URL. The Product acts as a bridge between Tableau and external systems such as communication tools and CRM platforms.

"we" or "our" implies Biztory, a limited liability company registered in Belgium, under number BE 0568.854.619, having its registered address at 2550 Kontich, Veldkant 31, Belgium.

If you have any questions, comments or complaints regarding this privacy statement or the processing of your personal data, or if you wish to exercise any of your rights, please contact us by email to E-MAILADRES PRIVACY.

1. Processing of Personal Data

This policy applies to personal data processed by the Biztory licensing infrastructure when the Product is activated or used. It does not apply to data that the Product sends to your own n8n webhook endpoint. That data is sent directly from the Viewer's browser – where a Viewer is a user who interacts with an existing Tableau dashboard without the ability to modify its configuration - to your systems and is entirely under your control as the dashboard author.

Since you act as the controller, you must comply with data protection laws, including GDPR, and ensure personal data processing is based on a lawful basis as outlined in Article 6 of the GDPR.

2. Why and how do we process your personal data?

The Product operates on a model where data processing takes place entirely within the user's environment. Autom8 does not have access to the content of the data transmitted via the extension between the connected systems, unless you expressly share this data as part of a support request.

2.1 Contact details customer

In connection with the conclusion and performance of the license agreement, Autom8 processes the following details of the customer's contact person(s):

- Surname and first name
- Professional email address
- Job title and company name
- Telephone number (if provided)

Legal basis: Performance of a contract (Article 6(1)(b) GDPR) — to communicate with the customer

Retention period: 7 years after the end of the agreement

2.2 Local browser storage

The Product stores a signed validation token (JWT) in the browser's localStorage on the device of each Viewer. This token contains:

- The license key identifier
- The licensed extension name
- An expiry timestamp

Why: To allow the Product to continue functioning for up to 72 hours if the Biztory licensing service is temporarily unreachable ("grace period").

Legal basis: Legitimate interest (Article 6(1)(f) GDPR) — ensuring continuity of a service already contracted for.

Retention period: Stored on the Viewer's device; expires after 72 hours or when the browser storage is cleared

2.3 License validation

When using the Extension, Autom8 generates an internal, random identifier (hereinafter: 'User ID') that is linked to the end user. This User ID is generated exclusively internally by the extension and is not derived from or linked to an identifier from the third-party platform. Every time the Product loads in a Tableau dashboard, it contacts the Biztory licensing service to verify the license key. The following data is sent and recorded:

- License key
- User identifier
- Tableau site ID
- Operational mode
- Webhook URL
- Timestamp
- Request count

Why: To enforce license validity, count unique monthly Viewers against your plan limit, and provide usage analytics in the customer portal.

Legal basis: Performance of a contract (Article 6(1)(b) GDPR) — license validation is necessary to provide the Product as purchased.

Retention period: Retained for the life of the license, then deleted within 90 days of license termination

2.4 Customer portal account

If you have a customer portal account, we hold:

- Your name and email address
- Your organisation name
- Your Cryptolens customer identifier (our license management provider)
- Activity timestamps

Why: To give you access to your license usage data and to manage your subscription.

Legal basis: Performance of a contract (Article 6(1)(b) GDPR).

Retention period: Retained while the account is active and for 2 years after account closure

3. Security of the Product

We implement robust technical and organizational measures to ensure the security of the migration process:

- **Encryption:** All data transfers via the Product are secured with strong encryption protocols (e.g., TLS) to prevent unauthorized access.
- **Automated processes:** The Product is designed to operate fully automatically, eliminating human access to your data.
- **Regular updates:** We regularly update the Product to ensure its security and functionality.
- **No storage:** Files or their contents are not stored on our servers.
- **Access control:** Access to your infrastructure is strictly limited to authorized personnel and is only granted for maintenance and support purposes upon your request.

4. Third Parties

We do not sell personal data. We share your personal data only with the following sub-processor:

Sub-processor	Purpose	Location
Cryptolens	License key management and validation	EU

Cryptolens receives the license key and product identifier for the purpose of verifying license validity. No user-identifying information is transmitted to Cryptolens.

5. Personal Data Breach

We take the security of our systems and your data very seriously. While the Product does not access or process the contents of your assets, we are committed to preventing unauthorized access, loss, or misuse of any data involved in the migration process, such as log files or metadata.

We will notify you without undue delay and no later than required of us by the GDPR, after we become aware of a personal data breach. We will promptly initiate an investigation into the circumstances surrounding the personal data breach and make its findings available to you.

Our obligation to report or respond to a personal data breach under this section is not an acknowledgement by us of any fault or liability with respect to the personal data breach. You must notify us promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Product.

6. International Transfers

Our licensing service and customer portal are operated within the European Economic Area. If data is transferred outside the EEA (for example, in connection with Cryptolens infrastructure), we ensure appropriate safeguards are in place, such as Standard Contractual Clauses approved by the European Commission.

7. Your Rights

We value your privacy and are committed to protecting any personal data we may access during the use of the Product. While we do not process the contents of your assets during normal operations, there are limited cases where we may access assets contents or user contact information, such as for technical support or related services. In these cases, the following rights apply:

1. Access and Correction:

- You have the right to request access to any personal data we may have processed in connection with providing technical support or storing your contact details.
- You may also request corrections to any inaccurate or incomplete personal data.

2. Data Deletion:

- You have the right to request that we delete any personal data, such as logs or support-related access, once it is no longer required for its original purpose, unless we are required to retain it by law.

3. Restriction of Processing:

- If you believe that your personal data is being processed in a way that you object to, you can request a temporary restriction while the matter is being reviewed.

4. Data Portability:

- Where applicable, you have the right to request a copy of your personal data in a structured, commonly used, and machine-readable format for transfer to another service provider.

5. Right to Object:

- You have the right to object to the processing of your personal data in the activities described in this policy. If you object to the processing of your personal data, we will no longer process the personal data unless we can demonstrate legitimate interests for processing that outweigh your interests, fundamental rights, and freedoms.

6. Right to Lodge a Complaint:

- If you believe we have not handled your data in accordance with this Privacy Policy or applicable laws, you have the right to lodge a complaint with the relevant data protection authority.

If you have any questions about your privacy rights or wish to exercise them, please contact us at [\[email address\]](#). We are committed to ensuring your privacy and security, even when providing technical support.

8. Changes to this Privacy Policy

We reserve the right to amend this Privacy Policy to reflect legal, technological, or operational changes. We encourage you to review this page regularly to stay informed about any changes.